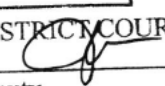



**SEALED**  
UNITED STATES DISTRICT COURT

for the  
Northern District of Texas

U.S. DISTRICT COURT  
NORTHERN DISTRICT OF TEXAS  
**FILED**  
JUL - 9 2018  
CLERK, U.S. DISTRICT COURT  
By  Deputy

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)  
2217 Cedar Crest Blvd, Dallas, TX 75203

Case No. 

**APPLICATION FOR A SEARCH WARRANT**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

(See Attachment A-2).

located in the Northern District of Texas, there is now concealed (identify the person or describe the property to be seized):

(See Attachment B).

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section*  
26 U.S.C. §§ 7201 and 7206 Tax Fraud  
(1)

*Offense Description*

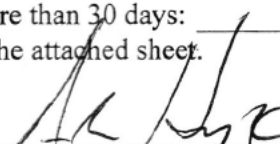
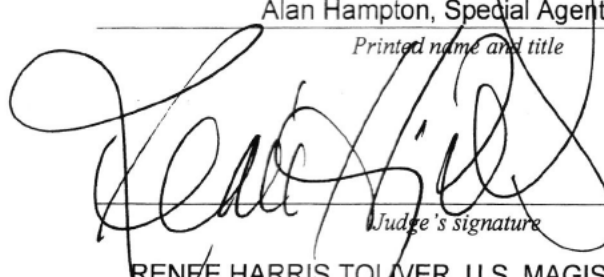
The application is based on these facts:

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of        days (give exact ending date if more than 30 days:       ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: 7/9/2018

City and state: Dallas, Texas

  
Applicant's signature  
Alan Hampton, Special Agent, IRS  
Printed name and title  
  
Judge's signature  
RENEE HARRIS TOLVER, U.S. MAGISTRATE JUDGE  
Printed name and title

**AFFIDAVIT**

I, Alan Hampton, being duly sworn, do state as follows:

**PREFACE**

1. This affidavit is made to support a search warrant for the residence/business, 1934 Argyle Avenue, Dallas, TX 75203 and the Caraway Campaign Headquarters office (listed as a business location on the 2013 Caraway US Individual Income Tax Return Schedule C portion - Dwaine Caraway Advertising and Consulting) address of 2217 Cedar Crest Blvd., Dallas, TX 75203. Dwaine Caraway (Caraway) was an elected Dallas City Council Member until term limits forced him out of office in 2015. He was re-elected in 2017. He also served as Mayor Pro Tem of Dallas in 2011, and serves in the same capacity currently. Caraway formed Dwaine Caraway Advertising and Consulting, LLC in June 2012 and began receiving payments from ELF Investments at or around the same time. Caraway received over \$400,000 in payments and according to his tax returns only reported \$240,000 in gross income from 2012 through 2015.
2. Based on my training, experience, and the information contained in the subsequent paragraphs, I believe there is probable cause that Caraway filed false tax returns and evaded US Individual Income Tax for the years 2012 through 2017 and that evidence related to Caraway's evasion of income tax scheme will be found at the above-referenced locations, and in support, I allege the following:

### INTRODUCTION

3. I am a Special Agent (SA) with the Internal Revenue Service, Criminal Investigation (CI), United States Department of the Treasury. I am assigned to the Dallas, Texas office and have been employed in this capacity since July 1991. My responsibilities include the investigation of possible criminal violations of the Internal Revenue Laws (Title 26, United States Code), the Bank Secrecy Act (Title 31, United States Code), the Money Laundering Control Act (Title 18, United States Code), and other related offenses. I am currently assigned to the Internal Revenue Service-Financial Crimes Investigative Task Force in Irving, Texas. Our mission is to identify and investigate possible money laundering and bank secrecy violations, specifically, violations of 18 U.S.C. §§ 1956, 1957, and 1960 and 31 U.S.C. §§ 5316, 5324, and 5330.

4. I have conducted, and assisted in conducting, numerous investigations involving allegations of one or more of the aforementioned financial crimes. I have also served as the affiant for several search and seizure warrants in prior financial investigations.

#### ***26 U.S.C. § 7201 (Attempt to Evade or Defeat Taxes)***

5. Section 7201 makes it a crime to willfully attempt in any manner to evade or defeat any tax under the Internal Revenue Code. To establish liability for tax evasion, the government must prove the following elements beyond a reasonable doubt: (1) additional tax due and owing (*i.e.*, the existence of a tax deficiency); (2)

an affirmative act of evasion or affirmative attempt to evade; and (3) willfulness.

An unlawful gain, as well as a lawful one, constitutes taxable income when its recipient has such control over it that, as a practical matter, he derives readily realizable economic value from it.

6. Filing a false return is the most common method of attempting to evade the assessment of a tax.

***26 U.S.C. § 7206(1) (Filing False Individual Tax Returns)***

7. Section 7206(1) makes it a crime to willfully file false income tax returns. To convict a defendant for false statement under 26 U.S.C. § 7206(1), the government must prove the following elements beyond a reasonable doubt: (1) the defendant made and subscribed a return, statement, or other document which was false and the return, statement, or other document contained a written declaration that it was made under the penalties of perjury; (2) the defendant did not believe the return, statement, or other document to be true and correct as to every material matter; and (3) the defendant falsely subscribed to the return, statement, or other document willfully.
8. Based on my training and experience and that of the other criminal investigators involved in this investigation, I have found that it is common practice in the business community for business entities, such as DCAC, to maintain business records at its place of business for the current year, as well as for an extended



period of time. Finally, IRS Publication 583 advises businesses to keep and maintain books and records for a time period of three to six years.

9. I know that the aforementioned financial crimes are crimes of concealment, motivated by profit and greed. As such, individuals engaged in this type of activity attempt to amass wealth and engage in expenditures in a manner designed to prevent detection by law enforcement officers.
10. Based on my training, experience and my participation in this investigation and other investigations involving individuals engaged in tax crimes, I know that individuals and/or businesses engaged in tax crimes often maintain documents and financial records for long periods of time, particularly when they are involved in ongoing criminal conduct over a long period of time. I also know that individuals and/or businesses keep some, if not all, of their records in electronic form, such as on a computer. I know that documents and records can be in the form of printed documents or stored in computer memory or on computer disks or other computer storage mediums, including cell phones and other “smart” computer devices.
11. There are many reasons why an individual will generally maintain records for long periods of time. *First*, the records will often seem innocuous because of their nature (e.g. financial, credit card and banking documents, travel documents, receipts, client lists, documents reflecting purchases of assets, personal calendars, check books, videotapes and photographs, utility records, ownership records, letters and notes, tax returns and financial records, escrow files, telephone bills,

keys to safe deposit boxes, packaging materials, computer hardware and software). *Second*, the individual may no longer realize he still possesses the records or may believe law enforcement could not obtain a search warrant to seize the evidence. *Third*, the individual may also be under the mistaken belief that he has deleted, hidden or further destroyed computer-related evidence, which in fact, may be retrievable by a trained forensic computer expert. *Fourth*, as discussed further below, a taxpayer is required to maintain tax records for a specified period of time. *Lastly*, it is common for individuals to set aside or store such records in various rooms of the residence or business (for example, records of a home business may be stored in another room not designated as the home office, such as the garage, attic, or storage building), and because they generally have no immediate need for the records, they are often forgotten. To law enforcement, however, all these items may have significance and relevance when considered in light of other evidence.

#### **PROPERTY FOR SEARCH**

This affidavit is made to obtain a search warrant for the following properties:

##### **1934 Argyle Avenue, Dallas, TX 75203**

12. 1934 Argyle Avenue is a one-story single-family residence with light colored brick residence located at the southeast corner of Argyle Avenue and Lanark Avenue. The residence has a white iron security gate in front of the main door and has a circular drive through the front yard area. There is white decorative iron

fencing around the entire rear perimeter of the property with a carport visible from outside the fence area. There is an alley that runs behind the residence. A photograph of the residence is included in Attachment A. DCAC is located and registered at this address for the 2012 tax year which was filed on April 15, 2013.

**2217 Cedar Crest Blvd, Dallas, TX 75203**

13. 2217 Cedar Crest is a one-story strip business sixplex with light colored brick located on the west side of Cedar Crest Blvd between Bonnie View Road on the north side and Surrey Avenue on the south side. It's the third storefront from the right or fourth from the left. The business has a white iron security gate in front of the main door and white iron burglar bars over the storefront glass window. There is a large blue sign that says DWAINÉ CARAWAY District 4 Neighborhood Information Center (214) 943-1020 on the storefront. A photograph of the Campaign Headquarters is included in Attachment A-2. DCAC is located at this address as Dwaine Caraway Advertising and Consulting on the Dwaine Caraway US Individual Income Tax Return, specifically on the Schedule C portion which notates location of the business, for the 2013 tax year which was filed on February 27, 2017.

[NOTHING FURTHER ON THIS PAGE].

**FACTS SUPPORTING PROBABLE CAUSE**

**Investigative Background**

14. I have participated in the investigation of the criminal activity described herein and have spoken with other agents involved in this and related investigations. I have also read the reports prepared in connection with this and the related investigations. I make this affidavit based, in part, on personal knowledge, and in part upon information and belief, derived from, among other things, oral and written reports made to me or other agents of the Internal Revenue Service and agents of the Federal Bureau of Investigation involved in this investigation and other related investigations. As a result, I am familiar with all aspects of this investigation. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

**Case Overview**

15. The United States Attorney's Office, Northern District of Texas, and the Federal Bureau of Investigation ("FBI"), have an existing criminal investigation of Caraway and others regarding potential violations of conspiracy to launder money (18 U.S.C. § 1956(h)), bribery (18 U.S.C. § 666), honest services wire fraud (18 U.S.C. §§ 1343 & 1346), and Title 26 tax violations.
16. The investigation involves alleged corruption within the Dallas County Schools, a governmental entity, including payments made to officials in return for backing

the purchase of a school bus red light monitoring system and also alleged corruption involving payments to officially influence low income housing developments. Caraway is one of many co-conspirators that are being investigated and are involved in the alleged public corruption related offenses.

**SCHOOL BUS CAMERA PROGRAM**

17. Dallas County Schools' ("DCS") primary responsibility is the operation of its bus system, which transports approximately 75,000 children to and from school each day for a number of independent school districts located in Dallas County, Texas, and elsewhere in the State of Texas. DCS is the 4<sup>th</sup> largest pupil transportation organization in the country.

18. In 2008, DCS issued a Request for Proposal ("RFP") to find a vendor that could replace existing technology on DCS buses, and also help DCS deploy a digital audio/video recording solution that would be upgradable in the future. A growing trend in the pupil transportation industry at that time was the ability to issue citations to drivers that illegally passed a school bus once the stop arm was engaged through the use of video monitoring systems. The standard practice for similar stop arm camera programs was for the contractor to put cameras on 20-30% of the stop arms of the buses that traveled routes with the most safety violations free of charge, then share a percentage of the fines levied with the school district. DCS's request was unique in that DCS wanted to outfit all 1900 of its buses with the technology to record and monitor stop arm violations and

purchase the equipment to do so outright. Force Multiplier Solutions (“FXS”) replied to the proposal. FXS is owned and operated by Robert Leonard (“Leonard”).

19. In July 2009, DCS agreed to purchase all equipment from FXS. FXS agreed to install the equipment and software, create an operations center, and oversee all remote and on-site maintenance required to sustain the school bus monitoring systems. In September 2011, DCS and FXS officially entered into a one-year contract that provided both entities the capability of extending the contract another five years. On November 8, 2011, DCS remitted its initial purchase order worth approximately \$6 million as an advanced partial payment to FXS. This was followed up on November 9, 2011, by an initial payment by DCS via check to FXS of approximately \$2 million.

20. In July 2012, DCS and FXS agreed to extend their contract for the full five years outlined in the initial agreement. The exact financial terms of the contracts signed between DCS and FXS are unknown since the contracts do not explicitly state the financial obligation to which DCS is agreeing; however, six bonds were issued and the total amount of the contracts between DCS and FXS appears to be \$70 million.

21. Leonard and others participated in a bribery scheme to have the school bus camera project funded and then extended. To abet and conceal the scheme, companies were established with no apparent purpose other than to disguise the

flow of payments from Leonard to the principals responsible for the awarding of the bus cameras contract. Among these companies was ELF Investments (“ELF”). ELF was used as a layering corporation to disguise funds paid to Caraway, as well as DCS’s superintendent, Rick Sorrels, who entered into the contracts with FXS. ELF was funded by FXS and operated by Slater Swartwood (“Swartwood”), an FXS employee.

22. In exchange for the payments he received, Caraway voted on ordinances and authorizations in a way that forwarded FXS’s business interests, pressured the Dallas City Attorney’s Office to provide a favorable opinion about the propriety of fines associated with FXS’s stop-arm camera program, and promised to use his official position if and when necessary to forward Leonard’s efforts to develop low income housing.

*Low Income Housing Kickbacks*

23. Under the Low Income Housing Tax Credit program (“LIHTC”), the federal government allots \$9 billion a year in tax credits to state housing agencies based on state populations. Then the agencies distribute credits to selected housing developers based on a complex and bureaucratic process. Developers who receive credits usually sell them to large banks and other investors, often using syndication firms as intermediaries. This provides cash to developers for construction and gives investors equity in the projects, as well as credits to use on their tax returns over a 10 year period.

24. The Dallas Land Bank program allows the City of Dallas to seize properties that are undeveloped or in arrears on back taxes.

25. Once the properties are seized, Dallas makes the properties available for sale to developers who will in turn develop the properties and sell the housing to primarily low income families. The tax credits associated with the development of low income housing are considered to be very valuable. Access to these properties can be lucrative and are therefore highly sought. Caraway, in return for cash and other benefits, agreed to provide official support to potential developers of low income housing in the City of Dallas.

**Undercover Agent**

26. An FBI undercover agent (“UCA”) posed as an interested developer for low income housing and met with Caraway at Campaign HQ in January, March, and May of 2017. The UCA described Campaign HQ as a two room office space with a desk in the front room and Caraway’s desk and computer in the back room.

27. The UCA was introduced to Caraway for the purpose of helping the UCA receive investment property from the Dallas Land Bank. The UCA paid Caraway inducements to help the UCA develop low income housing in 2016 and 2017 totaling approximately \$50,000. This income does not appear to have been fully reported by Caraway on his 2016 and 2017 tax returns.



**DWAINE CARAWAY**

28. Caraway was a member of the Dallas City Council from 2011 through 2015. As part of his duties, he voted on DCS matters and also had the ability to influence decisions and vote on matters involving the Dallas Land Bank program.

**City Council Income**

29. As a council member, Caraway earned in the range of \$13,362 to \$34,003 a year.

The City of Dallas submitted Forms W-2 to Caraway in each of those years showing the amount earned and the amount of federal taxes withheld, among other things. Caraway filed returns for each of those years on the dates shown below and with the City of Dallas yearly totals:

| <u>Year</u> | <u>Date Filed</u> | <u>City Council Wages</u> |
|-------------|-------------------|---------------------------|
| 2012        | 4/15/2013         | \$34,003.00               |
| 2013        | 2/27/2017         | \$32,169.00               |
| 2014        | 2/27/2017         | \$31,940.00               |
| 2015        | 6/28/2017         | \$13,362.00               |

**Dwaine Caraway Advertising and Consulting, LLC (DCAC)**

**Corporation and Income**

30. Caraway registered DCAC as a Texas corporation on June 5, 2012, approximately one month before he received his first payment from ELF. Caraway was listed as the sole owner, president, and registered agent. The address listed was 1934 Argyle Avenue, Dallas, TX 75203. The State of Texas Certificate of Formation

document filing number is 801607286. Public records database inquiries reflect Caraway as the registered agent as of 3/17/2017. Public records database also reflect Dwaine Caraway as the president of the company as of 3/7/2018.

31. On July 2, 2012, Caraway opened two bank accounts at Wells Fargo. Wells Fargo account #5789609715 (WF9715), titled Dwaine Caraway Advertising and Consulting–Gold Business Services Package, was opened as the main account and Wells Fargo account #9740447637 (WF7637), titled Dwaine Caraway Advertising and Consulting–Business Market Rate Savings, was opened as a Business savings account.

**UNREPORTED INCOME TO CARAWAY**

32. Caraway was paid over \$400,000 during tax years 2012 through 2015, the vast majority of which went into DCAC bank accounts. This money was in addition to any remuneration he received as part of his Dallas City Council duties. All the money paid to Caraway originated from Robert Leonard or one of his companies, primarily FXS, which was awarded the DCS stop arm camera contract. Funds were generally routed from FXS through ELF which according to Swartwood did not have any other business purpose except to receive money from FXS and forward it to Caraway and others at the request of Leonard.
33. Leonard has confirmed that the payments to Caraway were an inducement for Caraway's favorable official actions, including voting on DCS related matters on

the city council, and for Caraway to officially support any low income projects that Leonard might pursue in the City of Dallas.

34. Financial records and other documentary evidence shows Caraway received at least \$105,000 in 2012, \$206,700 in 2013, \$87,000 in 2014, and \$22,423 in 2015 from Leonard. This additional income paid to Caraway does not appear to have been fully reported on Caraway's personal income tax returns for tax years 2012 through 2015. Accordingly, there is probable cause to believe the scheme violated 18 U.S.C. 26 §§ 7201 and 7206(1).

35. The Wells Fargo signature card lists Caraway as the sole owner of the relevant accounts titled and the Employer Identification Number (EIN) as 45-5440159. Additionally, the listed address for the accounts is 1934 Argyle Ave Dallas TX 75203, which is Caraway's residence.

36. The initial deposit into WF9715 is a \$15,000.00 check from ELF Investments LLC in Kenwood, CA. The memo line reads "As Per Agreement". As mentioned above, ELF Investments is owned by Slater Swartwood, who is also an employee of Busguard, LLC which was later renamed Force Multiplier Solutions (FXS). Caraway was retained as a "business consultant" by ELF in an agreement signed on July 1, 2012.

37. Caraway received regular monthly payments from ELF of \$15,000.00 beginning with that initial deposit through May 2014 when the relationship was terminated. He also received \$10,000.00 checks from ELF on July 17, 2012 and September

25, 2013. Caraway also received two additional payments from ELF of \$5,000 on July 17, 2014 and August 1, 2014. Additionally, Caraway also received other payments and benefits from Leonard or FXS.

38. Leonard also paid for Caraway's personal expenses on a few occasions. Notably \$3,000 for security cameras on March 20, 2013 and a flight to New Orleans for \$443.60 on April 5, 2013.

39. As a registered Texas corporation, DCAC is required to file corporate tax returns. However, Caraway chose to report income received from DCAC as a Schedule C sole proprietorship. This income should have been included as a schedule within the US Individual Income Tax Return filed by Caraway. The chart below displays the reported gross receipts reported on Caraway's Form 1040 for the 2012 to 2015 tax years versus the approximate amount of actual income received.

| <u>Year</u> | <u>Sch C Gross<br/>Receipts<br/>REPORTED<br/>RECEIPTS</u> | <u>Approximate<br/>Actual Income<br/>Received<br/>ACTUAL<br/>RECEIPTS</u> | <u>Difference</u> |
|-------------|---|---|-------------------|
| <b>2012</b> | \$60,000  | \$105,000   | \$45,000          |
| <b>2013</b> | \$180,000   | \$206,700   | \$26,700          |
| <b>2014</b> | \$0   | \$87,000  | \$87,000          |

|              |           |           |           |
|--------------|-----------|-----------|-----------|
| <b>2015</b>  | \$0       | \$22,423  | \$22,423  |
| <b>Total</b> | \$240,000 | \$424,566 | \$184,556 |

Corporate Expenses

40. For the years 2012 and 2013, Caraway filed a Schedule C, a Profit or Loss from Business schedule with his US Individual Income Tax Returns claiming the gross receipts identified above. Caraway also claimed expenses to offset the gross receipts, which substantially lowered his taxable income. For the tax years 2014 and 2015, Caraway did not file a Schedule C nor any other form of business income returns for income received from ELF, FXS, or Leonard, nor did he otherwise claim any income from the same.

41. In 2012, Caraway claimed \$38,827 as expenses, including \$20,425 as a car and truck expense, \$5,052 as depreciation and 179 expenses, \$1,329 for insurance, \$2,500 for office expense, \$1,100 for supplies, \$1,461 for meals and entertainment, and \$3,340 as other expenses. Additionally, Caraway claimed a \$17,739 expense for home business use relating to his Argyle Ave. residence.

In 2013, Caraway claimed \$125,430.00 as expenses, as follows:

|                      |          |
|----------------------|----------|
| Advertising          | \$10,870 |
| Car and Truck        | \$17,400 |
| Commissions and Fees | \$ 5,500 |

|                               |          |
|-------------------------------|----------|
| Contract Labor                | \$26,000 |
| Insurance                     | \$ 2,180 |
| Legal and Professional        | \$ 6,500 |
| Office                        | \$10,150 |
| Rent -Other business property | \$ 4,800 |
| Repairs/Maintenance           | \$ 5,000 |
| Supplies                      | \$ 4,780 |
| Travel                        | \$ 7,200 |
| Meals and Entertainment       | \$ 3,750 |
| Utilities                     | \$ 3,900 |
| Other Expenses                | \$17,400 |

42. In analyzing the bank accounts associated with DCAC, I reviewed all of the deposits and withdrawals associated with both of the Wells Fargo accounts. The accounts appear to be used as depository accounts with the only money deposited being from ELF or transfers between the two accounts. A large portion of the money is withdrawn in cash. There are a few payments to a Bank of America home loan of \$986.03, payments to Lone Star Property Mgmt, which appear to be rent payments for his campaign HQ at 2217 Cedar Crest Blvd., four payments to Andrea Griffin totaling \$9,000, and a few miscellaneous personal expenses. In

general, DCAC, based on my training and experience, does not appear to be incurring the normal and regular expenses of a legitimate business and business account.

#### **USE OF HOME AS BUSINESS**

43. For the 2012 year, Caraway filed a Form 8829, Expenses for Business Use of Your Home schedule, with his US Individual Income Tax Return. On this form, Caraway claimed approximately 13% of his home solely for business use. During this year all bank records and other business filings reflect the Argyle Ave. address as the business address for DCAC. For 2013 tax return, Caraway listed his campaign office located at 2217 Cedar Crest Blvd, Dallas, TX 75201, as the business address of DCAC. Bank records for all subsequent years continue to list the Argyle Ave. address as the business address, including the address provided on his 2014 and 2015 tax returns that were filed in 2017.

#### **USE OF CAMPAIGN HQ AS BUSINESS**

44. The Caraway Campaign HQ at 2217 Cedar Crest Blvd., Dallas TX 75203 was also listed as the business location on the 2013 Caraway US Individual Income Tax Return on the Schedule C which lists the revenues and expenses for DCAC. 2013 is the last year that Caraway notes any type of business activity for DCAC on his tax returns, even though he received at least \$22,000 in 2015. Caraway met with UC agents at the Cedar Crest address and took money intended to influence decisions in which he participated in the Dallas City Council in the 2016 tax year.

45. Bank and other mailing's records show the Caraway campaign accounts are currently receiving statements at the 2217 Cedar Crest Blvd address. Utilities are also active at the address and being paid by the Caraway Campaign.

### **IRS RECORD KEEPING REQUIREMENT**

#### **26 § 6001.**

##### **Notice or regulations requiring records, statements, and special returns**

Every person liable for any tax imposed by this title, or for the collection thereof, shall keep such records, render such statements, make such returns, and comply with such rules and regulations as the Secretary may from time to time prescribe. Whenever in the judgment of the Secretary it is necessary, he may require any person, by notice served upon such person or by regulations, to make such returns, render such statements, or keep such records, as the Secretary deems sufficient to show whether or not such person is liable for tax under this title. The only records which an employer shall be required to keep under this section in connection with charged tips shall be charge receipts, records necessary to comply with section 6053(c), and copies of statements furnished by employees under section 6053(a).

The IRS has certain limits on how long a taxpayer may be audited. The general limitations period is three years, and an audit for willful conduct is six years.

Therefore, since the 2012 return was filed in 2013 we can reasonably expect business records for the tax year to be maintained through approximately 2019.

46. As this is a Schedule C business and not a corporation, records related to the business transactions of DCAC cannot be obtained by any civil procedure available to the IRS. Through my experience and other IRS Special Agents, it has been found that when an individual is engaged in a scheme to evade income taxes by under reporting business receipts, the books and records of the involved entity are rarely, if ever, produced upon request. It is, therefore, reasonable to conclude, and I do conclude, that the electronic data and all other records and documents



maintained by Caraway related to DCAC, necessary to establish the criminal offenses against the United States will be destroyed or otherwise placed beyond the reach of the government if a warrant to search the residence/business premises of Caraway and DCAC and seize those records is not executed.

#### **CELL PHONES and COMPUTERS**

47. Numerous interviews with Leonard, Swartwood, and Leonard's office manager, Elizabeth Michener confirm that Caraway communicated via email in receiving payments from Leonard through Swartwood and his company, ELF.

48. In numerous interviews, Leonard has stated he had contact with Caraway from as many as five different cell phone numbers. These cell phone communiques have been through text exchanges as well as voice mails and telephone conversations.

#### **DOCUMENTARY AND ELECTRONIC RECORDS**

49. Based on my training, experience, knowledge and participation in this and other criminal investigations, and accumulated knowledge from consultations with other law enforcement agents, including debriefings and interviews of known offenders in other cases, I also know and contend that the following traits are common practices of offenders involved in various types of fraud:

- a. fraud is frequently a continuing activity over months and years;

[NOTHING FURTHER ON THIS PAGE].

- b. offenders who commit fraud keep records of their illegal activities for a lengthy period of time, even extending substantially beyond the time during which they actually produce, market, sell, and profit from their crimes;
- c. offenders who commit fraud commonly maintain hard copy and computer files, books, records, receipts, notes, ledgers, journals, diaries, address books, and other sundry materials, and papers relating to their crimes; and
- d. Offenders who commit fraud often possess evidence, fruits, and instrumentalities relating to such offenses in their places of business, including home offices.

50. I am aware that people frequently use both business and personal cellular telephones (commonly called cell phones) for personal and professional communications and purposes. Many cell phones have advanced capabilities, including: internet browsing, text and e-mail, photography and video storage, notes, calendars, and data file storage. I am also aware, through training and experience, that people use cell phones to communicate with each other via voice, direct connect, text message, and e-mail; store valuable data such as names, and addresses; obtain and store directions and maps; search the Internet; and, capture audio, image, and video files.

51. As described above, this affidavit is being submitted in support of search warrants for records that might be found on the "PREMISES" of 1934 Argyle Drive, Dallas, TX 75203, as described in Attachment A, and 2217 Cedar Crest Blvd, Dallas, TX 75203, as described in Attachment A-2, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive (including a server, such as an email server) or other storage media, including "smart" cellular telephones. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Federal Rule of Criminal Procedure 41(e)(2)(B).

52. Upon arriving at the PREMISES, the agents will attempt to create an electronic "image" of the computer. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Imaging a computer permits the agents to obtain an exact copy of the computer's stored data without actually seizing the computer hardware. The agents or qualified computer experts will then conduct an off-site search for only the things described in the warrant from the "mirror image" copy at a later date.

53. I submit that if a computer or storage medium is found on the premises there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- e. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years

after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

f. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

g. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

h. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

54. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the premises of 1934 Argyle Avenue, Dallas, TX 75203, as described in Attachment A and 2217 Cedar Crest Blvd. Dallas, TX 75203, as described in Attachment A-2 because:

i. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence

in which they were created, although this information can later be falsified.

j. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, and electronic storage media that connected with the computer and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the

chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

[NOTHING FURTHER ON THIS PAGE].

k. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

l. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

m. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

55. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the



premises, it is sometimes possible to make an image copy of storage media.

Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

n. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

o. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will

be required to analyze the system and its data at the search location. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

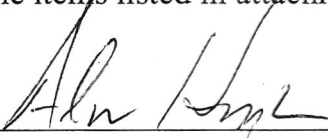
p. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

56. Based on the foregoing, and consistent with Federal Rule of Criminal Procedure 41(e) (2) (B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

### **CONCLUSION**

57. Caraway was paid over \$400,000 from Leonard, FXS, or associated entities and individuals during tax years 2012 through 2016. Caraway received at least \$105,000 in 2012, \$206,700 in 2013, \$87,000 in 2014, \$22,423 in 2015, and \$25,000 in 2016. The income does not appear to have been fully reported on Caraway's tax returns for tax years 2012 through 2016. Although we have good evidence to show the amount of income, the expenses reported on the 2012 and 2013 appear dubious at best.

Additionally, there may be evidence of expenses for the 2014 and 2015 years in which DCAC income was entirely omitted. In addition, Caraway received over \$50,000 in UC payments in 2016 and 2017, which amounts were not fully reported on his tax returns. Based on my training, experience, and the information in the preceding paragraphs, there is probable cause to believe the evidence, fruits, and instrumentalities of violations of 26 U.S.C. §§ 7201 and 7206 (1) are located at the premises of 1934 Argyle Drive, Dallas, TX 75203, as described in Attachment A, and 2217 Cedar Crest Blvd., Dallas, TX 75203 as described in Attachment A-2. Your affiant, therefore, respectfully, requests that the attached warrant be issued authorizing the search and seizure of the items listed in attachment B.

  
\_\_\_\_\_  
Alan Hampton  
Special Agent  
IRS Criminal Investigation Division

Subscribed to and sworn before me on this 9 day of July, 2018.

  
\_\_\_\_\_  
RENEE HARRIS TOLIVER  
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-2



## **ATTACHMENT B**

### **Items to be Seized**

Based on the information contained in this affidavit, I respectfully submit that there is probable cause to seize the following items which constitute evidence, fruits, and instrumentalities of 26, United States Code, § 7201 and 7206(1):

1. The following records are to be seized;
2. For the entities Caraway Advertising and Consulting LLC, and the individuals Dwaine Caraway for the time period January 2012 to present:

A. Upon arriving at the PREMISES, the agents will attempt to create an electronic "image" of the computer. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Imaging a computer permits the agents to obtain an exact copy of the computer's stored data without actually seizing the computer hardware. The agents or qualified computer experts will then conduct an off-site search for only the things described in the warrant from the "mirror image" copy at a later date.

B. Records, including electronic communication (i.e., e-mail, text message), concerning or relating to any promise to pay a monetary obligation, including but not limited to open or closed loans, notes, promissory notes, mortgages, mortgage notes, negotiable instruments, letters of credit or any other credit facilities, deeds of trust or other security instruments, loan agreements, participation agreements, loan applications (whether

pending, accepted, or rejected), correspondence, checks or deposit items representing the disbursement of principal, collateral ledgers, guarantees, cash flow analysis and projection, interest rate analysis, blended rate analysis, pro formas, loan narratives, appraisals, absorptions, audits, certifications, and loan assignments, modifications, amendments, or terminations;

C. Records, including electronic communication (i.e., e-mail, text message) relating to or concerning invoices, receipts, statements, cancelled checks, general ledgers, trial balances, spreadsheets, correspondence with creditors, credit card transactions, payroll transactions, loans, cash flow analysis, cash flow projection, pro formas, loan narratives, appraisals, collateral, financial analysis, absorptions, audits, certifications, and drafts, filings, and correspondence with the United States Securities and Exchange Commission (SEC);

D. Memoranda, notes, files, videotapes, audiotapes, agendas, and other documents, including electronic communication (i.e., e-mail, text message), relating to any meeting of Sorrells, Leonard, and government officials relating to Dallas County Schools or Force Multiplier Solutions.

E. Records, including electronic communication (i.e., e-mail, text message), relating to or concerning any contracts involving the above-listed entities and third party brokers;

F. Personnel files relating to or concerning any of the executives, officers, employees, and agents of Dallas County Schools and Force Multiplier Solutions.

G. Records, including electronic communication (i.e., e-mail, text message), relating to or concerning any open or closed bank account (whether savings, checking, or other type of account), such records to include periodic account statements, corporate resolutions, partnership agreements, customer ledgers, income tax returns, deposit tickets, cancelled checks, signature cards, account opening documents, and any and all correspondence;

H. Other bank records, including money orders, cashier's checks, and drafts, with application or requisition forms, certified checks, wire transfers, insurance records, safe deposit box records, or copies of any negotiable instruments cashed or paid by the bank without entry to any depository account.

I. Memoranda, notes, files, videotapes, audiotapes, agendas, and other documents, including electronic communication (i.e., e-mail, text message), relating to ELF Investments.

J. Computers and computer related evidence, as follows:

- a. Computer storage media and related hardware, including any computer hard drives, floppy disks, CDs or other electronic storage media including "smart" cellular telephones in which any files and records to be searched for may by

located. The agents executing this search warrant are authorized to seize, where necessary, the computer system's CPU, input/output ("I/O") or peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately reproduce the system set-up and retrieve the system's data in a laboratory or other controlled environment;<sup>1</sup> and

- b. Computer software, meaning any and all instructions or programs stored either in the form of hard copy or in electronic or magnetic media that are capable of being interpreted by a computer or related component. The items to be seized include operating systems, application software, utility programs, compilers, interpreters, and other programs or software used to communicate with computer hardware or peripherals either directly or indirectly via telephone lines, radio, or other means of transmission.

K. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

---

<sup>1</sup> If, after inspecting the I/O devices, software, documentation, and data security devices, the computer analyst determines that these items are no longer necessary to retrieve and preserve evidence, they will be returned within a reasonable time.



- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or

similar containers for electronic evidence;

- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.